Example 85. Recall that **Fermat's last theorem** states that $x^n + y^n = z^n$ does not have any solutions in positive integers if $n \geqslant 3$.

However, in a Simpson's episode, Homer discovered that

$$1782^{12} + 1841^{12} \text{ “=” } 1922^{12}.$$

If you check this on an old calculator it might confirm the equation. However, the equation is not correct, though it is "nearly": $1782^{12} + 1841^{12} - 1922^{12} \approx -7.002 \cdot 10^{29}$.

Why would that count as "nearly"? Well, the smallest of the three numbers is $1782^{12} \approx 1.025 \cdot 10^{39}$ is bigger by a factor of more than 10^9. So the difference is extremely small in comparison.

Relative errors. If you estimate x with y, the **absolute error** is $|x - y|$. However, for many applications, the **relative error** $\left|\frac{x-y}{x}\right|$ is much more important.

Show that Homer is wrong by hand! Hint: look at this modulo 13.

Solution. By Fermat's little theorem, we have $x^{12} \equiv 1 \pmod{13}$ for all x not divisible by 13. Our numbers are not divisible by 13. Hence, $1782^{12} + 1841^{12} \equiv 2 \pmod{13}$ but $1922^{12} \equiv 1 \pmod{13}$, so they cannot be equal.

http://www.bbc.com/news/magazine-24724635

Example 86. (bonus challenge) Find the factors of the following number $M = pq$:

89320280057437363393608386387469360495079915773073599087435569428108 27\
07615146116506918133536640188765047775335776026093439165454319252186 33\
75114106509563452970373049082933244013107347141654282924032714311

As indicated in Example 80, this is difficult. Through some sort of espionage, however, you have learned that $\phi(M)$ is:

89320280057437363393608386387469360495079915773073599087435569428108 27\
07615146116506918133536640188675726495278338662699830779066849891691 25\
75956375773572578614678768000225628866990840223520746283867797512

In general, if $M = pq$ is a product of two large primes p, q, given $\phi(M)$, how can we factor M?

Comment. Even if we don't know the number of prime factors of M (in the above case we know that M is a product of two primes), we can "efficiently" factor M if we know the value of $\phi(M)$.

How many primes are there?

Theorem 87. (Euclid) There are infinitely many primes.

Proof. Assume (for contradiction) there is only finitely many primes: $p_1, p_2, \ldots, p_n$.
Consider the number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
None of the p_i divide N (because division of N by any p_i leaves remainder 1).
Thus any prime dividing N is not on our list. Contradiction.

Just being silly. Similarly, there are infinitely many composite numbers.

Indeed, assume (for contradiction) there is only finitely many composites: $m_1, m_2, \ldots, m_n$.
Consider the number $N = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ (don't add 1).
N is not on our list. Contradiction. □

Armin Straub
straub@southalabama.edu

The following two famous results say a bit more about the infinitude of primes.

- **Bertrand's postulate**: for every $n>1$, the interval $(n,2n)$ contains at least one prime.

  conjectured by Bertrand in 1845 (he checked up to $n=3\cdot 10^6$), proved by Chebyshev in 1852

- **Prime number theorem**: up to x, there are roughly $x/\ln(x)$ many primes

  proportion of primes up to 10^6: $\frac{78,498}{10^6}=7.850\%$ vs $\frac{1}{\ln(10^6)}=\frac{1}{6\ln(10)}=7.238\%$

  proportion of primes up to 10^9: $\frac{50,847,534}{10^9}=5.085\%$ vs $\frac{1}{\ln(10^9)}=4.825\%$

  proportion of primes up to 10^{12}: $\frac{37,607,912,018}{10^{12}}=3.761\%$ vs $\frac{1}{\ln(10^{12})}=3.619\%$

  Of huge relevance for crypto.

  The estimated proportion of primes up to 2^{2048} is $\frac{1}{\ln(2^{2048})}=0.0704\%$.

  That means, roughly, 1 in 1500 numbers of this magnitude is prime. That means we (i.e. our computer) can efficiently generate large random primes by just repeatedly generating large random numbers and discarding those that are not prime.

  Comment. Here, $\ln(x)$ is the logarithm with base e. Isn't it wonderful how Euler's number $e\approx 2.71828$ is sneaking up on the primes?

Example 88. (extra) What can you say about factors of $n!+1$? Is $n!+1$ composite infinitely often. Is it prime infinitely often?

Solution.

n	1	2	3	4	5	6	7	8	9	10	11	12
$n!+1$	2	3	7	5^2	11^2	$7\cdot 103$	71^2	$61\cdot 661$	$19\cdot 71\cdot 269$	$11\cdot 329,891$	$39,916,801$	$13^2\cdot 2,834,329$

- Every factor $m\geqslant 2$ of $n!+1$ has to be bigger than n. That's because, if $m\leqslant n$, then $n!+1\equiv 1 \pmod m$.

  Comment. In other words, the number $n!+1$ has the property that all its prime factors are bigger than n. This observation provides us with another proof that there is infinitely many primes (see below).

- By Wilson's theorem (which we discuss below), if p is a prime, then p divides $(p-1)!+1$. Hence, $n!+1$ is composite whenever $n+1$ is prime (so that $n=p-1$ for some prime p).

- It is not known whether $n!+1$ is prime infinitely often. $n!+1$ is prime for $n=1,2,3,11,27,37,41,73,77,116,\ldots$. The largest such value known (proven in 2000) is $n=6380$.

  Comment. As of Feb 2018, $150209!+1$ is the 756th largest known prime number (it has $712,355$ decimal digits). For comparison, the largest known prime is $2^{77,232,917}-1$ (a Mersenne prime; like the last 16 record primes). It has a bit over 23.2 million (decimal) digits.

Another proof of Euclid's theorem. In order to show that there are infinitely many primes, it is sufficient to observe that there doesn't exist a largest prime number. But, as noted above, the number $n!+1$ has the property that all its prime factors are bigger than n, so that arbitrarily large primes exist.